



U.S. Department of the Interior PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the [DOI PIA Guide](#) for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: eMail Enterprise Records Document Management System (eERDMS)

Bureau/Office: Office of the Secretary

Date: September 30, 2019

Point of Contact

Name: Teri Barnett

Title: Departmental Privacy Officer

Email: DOI_Privacy@ios.doi.gov

Phone: 202-208-1605

Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on

☐ Members of the general public

☐ Federal personnel and/or Federal contractors

☐ Volunteers

☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Department of the Interior (DOI) eMail Enterprise Records Document Management System (eERDMS) helps DOI meet its objective to identify, acquire and deploy an enterprise application that combines electronic workflow, imaging, and management of documents, e-mails, discovery,



and records. eERDMS provides the framework for enterprise use for storing, accessing, and managing the DOI's records, regardless of format, media, source or location.

eERDMS is a major application that includes five sub-applications: Enterprise eArchive System (EES), Enterprise Content System (ECS), Early Case Assessment (ECA), Advanced Early Case Assessment (AECA) and OpenText Auto-Classification (OTAC). The EES, ECS, ECA, and AECA components contain personally identifiable information (PII) and the privacy implications for these components are assessed in this privacy impact assessment.

- EES provides a Department-wide email archival and document management capability to allow the Department to retain and protect email communication for the appropriate retention periods and to ensure that past and future emails and email attachments will be reliably, consistently and automatically captured, archived, and retained in a safe and secure environment.
- ECS manages non-email electronic content in support of the records management initiatives of DOI with an online centralized electronic document archive.
- ECA and AECA work together to manage collections created within ECS to support OMB Circular A-130 areas, e-Discovery, and internal investigations.
- OTAC is a component that temporarily pulls data from EES to process data. The only data that is stored in OTAC are statistical information and EES DataIDs.

The EES, ECS, and ECA/AECA in eERDMS provide the framework for storing, accessing, and managing the Department's records. DOI employees will have access to electronic records and documentation through a web browser to create, access and share information. As the rate of Information Technology (IT) change accelerates, there are increasing concerns about the government's ability to manage and preserve its records and to meet accountability and archival obligations. Using eERDMS as an enterprise solution allows DOI to address program specific concerns such as preventing the loss of records that should be kept for legal and accountability purposes, achieving confidence in the authenticity and reliability of records, eliminating confusion between record versions, maintaining context to understand records properly, and controlling and planning for technological change that could make records inaccessible or incomprehensible.

C. What is the legal authority?

- The Paperwork Reduction Act, 44 U.S.C. 3501
- The Clinger-Cohen Act of 1996, 40 U.S.C. 1401
- 36 CFR 1220: Federal Records, General
- OMB Circular A-130, *Managing Information as a Strategic Resource*
- Executive Order 13571, *Streamlining Service Delivery and Improving Customer Service*
- Presidential Memorandum, *Security Authorization of Information Systems in Cloud Computing Environments*
- Presidential Memorandum, *Building a 21st Century Digital Government*
- OMB M-12-18, *Managing Government Records*
- Presidential Memorandum, *Managing Government Records*



D. Why is this PIA being completed or modified?

- ☐ New Information System
- ☐ New Electronic Collection
- ☒ Existing Information System under Periodic Review
- ☐ Merging of Systems
- ☐ Significantly Modified Information System
- ☐ Conversion from Paper to Electronic Records
- ☐ Retiring or Decommissioning a System
- ☐ Other: *Describe*

E. Is this information system registered in CSAM?

- ☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

010-000001728; eMail Enterprise Records and Document and Management System (eERDMS)
SSP

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII (Yes/No)	Describe <i>If Yes, provide a description.</i>
Enterprise eArchive System (EES)	EES provides a Department-wide email archival and document management capability to allow the Department to retain and protect email communication for the appropriate retention periods and to ensure that past and future emails and email attachments will be reliably, consistently and automatically captured, archived and retained in a safe and secure environment.	Yes	Name, Personal Email of Email Sender and recipients, Personal Phone Number, Personal Address, Social Security Number, Tribal Identification Number, Date of Birth, Credit Card Number, Driver License Number, Vehicle Identification Number, License Plate Number, Identification Badge Data, Financial Information, Medical Information, Disability Status, Ethnicity, Race, Nationality, Physical or Distinguishing Attributes, Photos, Spouse or Dependent Information, Passport Number, Gender, Fingerprints, Hair and Eye Color, Biometric Data and other information found in email correspondence generated, maintained and



Subsystem Name	Purpose	Contains PII (Yes/No)	Describe <i>If Yes, provide a description.</i>
			received during the transactions and work activities of DOI bureaus, offices and programs.
Enterprise Content System (ECS)	ECS is used to manage online content in support of the records management initiatives of DOI with an online centralized electronic and document content capture and mobility management solution.	Yes	Name, Citizenship, Gender, Birth Date, Marital Status, Other Names Used, Truncated SSN, Legal Status, Place of Birth, Security Clearance, Spouse Information, Financial Information, Medical Information, Disability Information, Credit Card Number, Law Enforcement, Education Information, Emergency Contact, Driver's License, Race/Ethnicity, Social Security Number (SSN), Personal Cell Telephone Number, Tribal or Other ID Number, Personal Email Address, Mother's Maiden Name, Home Telephone Number, Child or Dependent Information, Employment Information, Military Status/Service and Mailing/Home Address
Early Case Assessment (ECA)/Advanced Early Case Assessment (AECA)	ECA manages collections created within ECS to support A-130 areas, e-Discovery and internal investigations. AECA is used to perform deep analysis of collections from the ECA process.	Yes	Name, Personal Email of Email Sender and recipients, Personal Phone Number, Personal Address, Social Security Number, Tribal Identification Number, Date of Birth, Credit Card Number, Driver License Number, Vehicle Identification Number, License Plate Number, Identification Badge Data, Financial Information, Medical Information, Disability Status, Ethnicity, Race, Nationality, Physical or Distinguishing Attributes, Photos, Spouse or Dependent Information, Passport Number, Gender, Fingerprints, Hair and Eye Color, Biometric Data and other information found in email correspondence generated, maintained and



Subsystem Name	Purpose	Contains PII (Yes/No)	Describe <i>If Yes, provide a description.</i>
			received during the transactions and work activities of DOI bureaus, offices and programs.
OpenText Auto-Classification (OTAC)	OTAC pulls in data from EES temporarily to process statistics.	No	

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

OS-10, Electronic Email Archive System (EEAS), 68 FR 4220 (January 28, 2003); modification published 73 FR 8342 (February 13, 2008). Due to the nature of eERDMS as DOI's enterprise records management system, records may be covered by Government-wide or DOI Privacy Act system of records which may be viewed at <https://www.doi.gov/privacy/sorn>.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*

☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

- ☒ Name
- ☒ Citizenship
- ☒ Gender
- ☒ Birth Date
- ☒ Group Affiliation
- ☒ Marital Status
- ☒ Biometrics
- ☒ Other Names Used
- ☒ Truncated SSN
- ☒ Legal Status
- ☒ Place of Birth
- ☒ Religious Preference



- ☒ Security Clearance
- ☒ Spouse Information
- ☒ Financial Information
- ☒ Medical Information
- ☒ Disability Information
- ☒ Credit Card Number
- ☒ Law Enforcement
- ☒ Education Information
- ☒ Emergency Contact
- ☒ Driver's License
- ☒ Race/Ethnicity
- ☒ Social Security Number (SSN)
- ☒ Personal Cell Telephone Number
- ☒ Tribal or Other ID Number
- ☒ Personal Email Address
- ☒ Mother's Maiden Name
- ☒ Home Telephone Number
- ☒ Child or Dependent Information
- ☒ Employment Information
- ☒ Military Status/Service
- ☒ Mailing/Home Address
- ☒ Other: *Specify the PII collected.*

Due to the nature of eERDMS as DOI's enterprise records management system, records may include various types of PII or other information about individuals that is contained in DOI records. EES and ECS may collect any PII that a user chooses to include in an email or other electronic document that is stored for recordkeeping purposes. ECA/AECA are copies of documents pulled from EES, ECS or other sources which are used for document production purposes like Congressional Inquiries, Litigation Support, Freedom of Information Act (FOIA), etc.

B. What is the source for the PII collected? Indicate all that apply.

- ☒ Individual
- ☒ Federal agency
- ☒ Tribal agency
- ☒ Local agency
- ☒ DOI records
- ☒ Third party source
- ☒ State agency
- ☒ Other: *Describe*



EES and ECS may collect any PII that a user chooses to include in an email or other electronic document that is stored for record keeping purposes. ECA/AECA are copies of documents pulled from EES, ECS or other sources which are used for document production purposes like Congressional Inquiries, Litigation Support, FOIA, etc.

C. How will the information be collected? Indicate all that apply.

- ☒ Paper Format
- ☒ Email
- ☐ Face-to-Face Contact
- ☒ Web site
- ☐ Fax
- ☐ Telephone Interview
- ☒ Information Shared Between Systems
- ☒ Other: *Describe*

EES and ECS may collect any PII that a user chooses to include in an email or other electronic document that is stored for record keeping purposes. ECA/AECA are copies of documents pulled from EES, ECS or other sources which are used for document production purposes like Congressional Inquiries, Litigation Support, FOIA, etc.

D. What is the intended use of the PII collected?

The purpose of eERDMS is to provide a framework for enterprise use for storing, accessing, and managing the DOI's records. eERDMS allows DOI to address program specific concerns such as preventing the loss of records that should be kept for legal and accountability purposes, achieving confidence in the authenticity and reliability of records, eliminating confusion between record versions, maintaining context to understand records properly, and controlling and planning for technological change that could make records inaccessible or incomprehensible. PII contained in these records may be used as part of or in support of records management or records keeping purposes, to support audits, discovery, email and document management, and document production purposes like Congressional Inquiries, FOIA and litigation support.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

- ☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

The Office of the Chief Information Officer (OCIO) manages and maintains the eERDMS system. The Departmental Records Officer within the OCIO has access to all the records within the system, and may share information as requested.



EES and ECS may collect any PII that a user chooses to include in an email or other electronic document that is stored for record keeping purposes. Each bureau designates specific individuals records management functions that have access to these systems.

ECA/AECA are copies of documents pulled from EES, ECS or other sources which are used for document production purposes like Congressional Inquiries, Litigation Support, FOIA, etc. The Office of the Executive Secretariat and the Office of the Solicitor review document collections to determine what needs to be redacted and what is appropriate for release depending on the specific request.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

EES and ECS may collect any PII that a user chooses to include in an email or other electronic document that is stored for record keeping purposes. Each bureau designates specific individuals records management functions that have access to these systems.

ECA/AECA are copies of documents pulled from EES, ECS or other sources which are used for document production purposes like Congressional Inquiries, Litigation Support, FOIA, etc. The Office of the Executive Secretariat and the Office of the Solicitor review document collections to determine what needs to be redacted and what is appropriate for release depending on the specific request.

PII is shared with DOI employees, contractors, and volunteers who access the system through their DOI Active Directory account and is used to report key statistical transactional data related to eERDMS.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Other Federal Agencies do not access EES/ECS directly. However, ECA/AECA are copies of documents pulled from EES, ECS or other sources which are used for document production purposes like Congressional Inquiries, Litigation Support, FOIA, etc. The Office of the Executive Secretariat and the Office of the Solicitor review document collections to determine what needs to be redacted and what is appropriate for release depending on the specific request. Information may be shared with other Federal agencies as authorized and required to meet legal and reporting requirements.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Tribal, State, or Local Agencies do not access EES/ECS directly. ECA/AECA are copies of documents pulled from EES, ECS or other sources which are used for document production purposes like Congressional Inquiries, Litigation Support, FOIA, etc. The Office of the Executive Secretariat and the Office of the Solicitor review document collections to determine what needs to be redacted and what is appropriate for release depending on the specific request.



☒ Contractor: *Describe the contractor and how the data will be used.*

Information may be shared with contractors who provide support for these program activities.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

Any information provided to other sources from eERDMS will go through the DOI FOIA process prior to being released. PII and other sensitive information will be redacted by the FOIA team.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☐ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

☒ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

eERDMS is a records management system and does not collect PII directly from the individual. The eERDMS components do not provide individuals with an opportunity to decline to provide information in the records management process.

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement: *Describe each applicable format.*

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided to individuals through the publication of this privacy impact assessment and the related systems of records notices published in the Federal Register.

☐ Other: *Describe each applicable format.*

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

EES, ECS, and ECA/AECA data may be retrieved using various types of keyword searches. The search criteria used will depend on specific search needs, but may include personal identifiers such as name and email address. Other personal identifiers may also be used, at the discretion of the individual performing the search. When retrieving data all requests go through an audit



request form process with management approvals that ensure the searches are within appropriate need and scope.

- EES - Date range, sender or recipient email address or key word search
- ECS - metadata driven based on type of document stored, e.g., document number or title
- ECA/AECA - contents are driven by documents pulled from EES or ECS, e.g., date range, sender or recipient email address, keyword search, document number or title

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

EES, ECS, and ECA/AECA are enterprise-wide content management systems that are used for content and document management and assist the Department in complying with Federal recordkeeping requirements, responding to FOIA requests and Congressional requests for information, and responding to electronic discovery actions. Subject to regulations limiting the disclosure of information, reports that support the purposes listed in the previous paragraph may be produced concerning documents created by an individual or documents that include personal information about the individual, as well as, emails sent or received by an individual.

Audit reports can be produced to review the actions of authorized system users to determine if their use of the EES, ECS, and ECA/AECA systems and the data has been in accordance with all rules and procedures for the system. Only users with elevated rights can run audit reports.

Statistical reports generated for system maintenance generally do not contain sensitive PII.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

eERDMS is an enterprise records management system that captures the records of the Department and relies on the sourcing systems and processes to ensure that the information provided is accurate. Otherwise, documents captured are intended to be duplicates of the originals, and are not otherwise checked for accuracy.

B. How will data be checked for completeness?

eERDMS is an enterprise records management system that captures the records of the Department and relies on the sourcing systems and processes to ensure that the information provided is complete. Otherwise, documents captured are intended to be duplicates of the originals, and are not otherwise checked for completeness.



C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

eERDMS is an enterprise records management system that captures the records of the Department and relies on the sourcing systems and processes to ensure that the information provided is current. Otherwise, documents captured are intended to be duplicates of the originals, and are not otherwise checked for currency. Since eERDMS is a record keeping system, by definition, some of the information retained in various components is historical and not current due to the requirements of the Federal Record Act.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Retention periods for records captured by eERDMS or any of the components vary according to agency needs and specific subject matter, and are retained in accordance with applicable Departmental Records Schedule (DRS) authorities, as approved by the National Archives and Records Administration (NARA). Some records are currently treated as “unscheduled” while the applicable DRS component is awaiting NARA approval, and must be treated as permanent records until the DRS items are approved. Records retention periods may also be suspended by litigation holds, court orders, preservation notices, and similar issued by the Office of the Solicitor, the DOI or Bureau Records Officer, or other authorized official.

System administrator logs are covered by DRS 1.4.0013, System Maintenance and Use Records (DAA-0048-2013-0001-0013). These records have a temporary disposition and are cut off when superseded or obsolete. Records are destroyed no later than 3 years after cut-off.

Data in ECA/AECA is maintained under DRS 1.1.0003, Administration Records of Specific Temporary Value (DAA-0048-2013-0001-0003). These records have a temporary disposition and are cut off when the object or subject the records refer to is removed/discontinued/obsolete. Records are destroyed when no longer needed.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

With EES and ECS, records are disposed of in accordance with the applicable Departmental Records Schedule disposition authority, Departmental policy and referenced NARA guidelines. EES and ECS include the ability to automatically notify records managers about records that have passed their disposition date. These disposition reports allow for individual review and processing decision (carry out the destruction action). When records are disposed of via disposition, a Department of Defense secure delete is performed on the records. Unscheduled records will be maintained as permanent records within the system and cannot be destroyed until the DRS items are approved by NARA. Permanent records will be transferred to NARA for ongoing retention at their appropriate disposition time.



ECA/AECA do not have an automated retention functionality. Since ECA/AECA are used for document production purposes all records contained in these systems are considered copies of the original and need to be maintained for as long as the Congressional inquiry, FOIA request, litigation, or other oversight request remains active.

F. Briefly describe privacy risks and how information handling practices at each stage of the “information lifecycle” (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

eERDMS primary privacy risks include unauthorized access, unauthorized disclosure and misuse of the data in the system. These risks are addressed and mitigated through a variety of administrative and logical security controls. When retrieving data all requests go through an audit request form process with management approvals that ensure the searches are within appropriate need and scope.

User access is granted only to authorized individuals by system administrators, and users are granted access only to the data sets needed in order to perform their job duties; data set access is also governed and limited by each user’s email domain. Only authorized users are provided access to eERDMS using single sign-on and validated through the DOI Active Directory. Administrative access to EES, ECS, and ECA/AECA is granted only to authorized personnel on an official need-to-know basis. Unique administrator identification and authentication, least privileges and audit logs are utilized to ensure appropriate permissions and access levels. In many cases, administrators can be granted adequate rights to fulfill their duties without being given access to data in the system.

All users of DOI network resources, including contractors, must consent to rules of behavior and take annual end-user security, privacy and records training in order to obtain access to any DOI network resource. EES, ECS, and ECA/AECA administrators are also required to take computer security and privacy role-based training.

EES, ECS, ECA, and AECA have a hierarchical administration consisting of a Lead Administrator, and multiple Support Administrators who supervise administrators at the Department level, as well as DOI bureaus and offices. Bureau and Office Records Officers are responsible for controlling and monitoring access of authorized records staff who are given access to data for their Bureau or Office. Bureau/Office Administrators and authorized employees are only granted access to documents and data in EES, ECS, ECA, and AECA to the extent it is necessary for the performance of their job duties. Access procedures are further described in the eERDMS System Authorization and Accreditation (A&A) documentation and the system security plan.

Audit logs, access level restrictions, and least privileges are used to ensure users have access only to the data they are authorized to view, which serves as a control on unauthorized monitoring. In addition, firewalls and network security arrangements are built into the architecture of the system, and NIST guidelines and Departmental policies are implemented to ensure system and data security. System administrators will review the activities of the users to ensure that the system is not improperly used, including for unauthorized monitoring.



Access is restricted to only those individuals authorized by System Administrators on a need to know basis in order to perform their job duties consistent with the purposes of the system. This includes limiting authorized individuals' access to selected repositories of documents and data within the system, such as the authorized individual's bureau or office. Limitations on access are maintained through user login and authentication.

There is a risk that data from different sources may be aggregated and may provide more information about an individual. This data may become outdated or inaccurate. Mitigation occurs at the time of entry through data validation. Records are disposed based upon the records management schedule.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy. The provider will implement protections and controls to restrict access to unauthorized parties, as will be required to attain the necessary FedRAMP Authority to Operate (ATO). The provider will be required to submit security accreditation to attain the DOI ATO to ensure the vendor's system handles and stores sensitive information in accordance with Federal and DOI privacy and security standards.

There is a risk that individuals may not have notice regarding the collection of information, the purposes for collection or how the information will be used. Notice is provided through the publication of this privacy impact assessment.

The user traceability program can detect and through ad-hoc capabilities report unauthorized access attempts to files outside of an authorized user's permissions. The audit logs for the eERDMS components may be used to run reports on individual users' access to and actions within the system. The user traceability program can detect and report unauthorized access attempts to files outside of an authorized user's permissions.

With EES, due to the high volume of documents being added to EES, the system utilizes auto-classification technologies to classify and categorize email journaled to the solution. While this is a new technology, processes are being put in place so that statistical data and samples are reviewed by bureau records officers to ensure the auto-classification is maintained in as accurate a manner as possible.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

eERDMS enables DOI to manage and preserve its records and to meet accountability and archival obligations under the Federal Records Act. eERDMS allows DOI to address program



specific concerns such as preventing the loss of records that should be kept for legal and accountability purposes, achieving confidence in the authenticity and reliability of records, eliminating confusion between record versions, maintaining context to understand records properly, and controlling and planning for technological change that could make records inaccessible or incomprehensible.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*

☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*

☒ No

E. How will the new data be verified for relevance and accuracy?

Not applicable. eERDMS is a records and document management system that captures the records of the Department and will not derive new data or create previously unavailable data.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.



G. Who will have access to data in the system or electronic collection? Indicate all that apply.

- ☒ Users
- ☒ Contractors
- ☒ Developers
- ☒ System Administrator
- ☒ Other: *Describe*

Access to information will be limited to those authorized individuals that have a need to know the data in order to perform official duties, including system administrators, authorized program personnel, and contractors based on least privileges.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access level restrictions, authentication, least privileges, and audit logs are used to ensure users have access only to the data they are authorized to view. Access is further governed by DOI IT security policy, including use of assigned passwords, limited access rules, various firewalls, and other protections put in place to ensure the integrity and protection of information. All DOI employees and contractor employees undergo initial and annual security, privacy and records management training, and sign DOI Rules of Behavior before being granted access to DOI networks and information.

EES, ECS, ECA, and AECA have a hierarchical administration consisting of a Lead Administrator, and multiple Support Administrators who supervise administrators at the Department level, as well as DOI bureaus and offices. Bureau and Office Records Officers are responsible for controlling and monitoring access of authorized records staff who are given access to data for their Bureau or Office. Bureau/Office Administrators and authorized employees are only granted access to documents and data in EES, ECS, ECA, and AECA to the extent it is necessary for the performance of their job duties. Access procedures are further described in the eERDMS System Authorization and Accreditation (A&A) documentation and the system security plan.

Access is restricted to only those individuals authorized by System Administrators on a need to know basis in order to perform their job duties consistent with the purposes of the system. This includes limiting authorized individuals' access to selected repositories of documents and data within the system, such as the authorized individual's bureau or office. Limitations on access are maintained through user login and authentication.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

- ☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*



Contractors were involved with the design and configuration of the system and will be involved with the maintenance and operation of the system. Federal Acquisition Regulation (FAR) contract Clause 52.224-1, Privacy Act Notification (April 1984), FAR contract Clause 52.224-2, Privacy Act (April 1984), FAR contract Clause 52.239-1, Privacy or Security Safeguards (August 1996) and 5 U.S.C. 552a are included by reference in the agreement with the contractor.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

eERDMS is not intended to monitor individuals. However, the system has the ability to audit usage of the system, including reviewable data concerning logins, including login time, to protect against unauthorized access or actions within the system. Audit logs, access level restrictions, and least privileges are used to ensure users have access only to the data they are authorized to view, which serves as a control on unauthorized monitoring. In addition, firewalls and network security arrangements are built into the architecture of the system, and NIST guidelines and Departmental policies are implemented to ensure system and data security. System administrators will review the activities of the users to ensure that the system is not improperly used, including for unauthorized monitoring.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

eERDMS is not intended to monitor individuals. However, the system has the ability to audit usage of the system, including use by authorized individuals and system administrators. This includes reviewable data concerning actions within the system, including username, date and time of day a user accessed the system, specific uniform resource locators (URLs) of component systems, search terms or parameters used to call data, user creation and deletion of files, user creation or deletion of user accounts, and changes to account privileges. The user traceability program can detect and through ad-hoc capabilities report unauthorized access attempts to files outside of an authorized user's permissions.

The eERDMS audit logs can be used to run reports on individual users' access to and actions within the system, including username, date and time of day a user accessed the system, specific URLs of system web pages and documents accessed, search terms or parameters used to call data from the databases, user creation and deletion of files, user creation or deletion of user accounts, and changes to account privileges. The user traceability program can detect and report unauthorized access attempts to files outside of an authorized user's permissions.



M. What controls will be used to prevent unauthorized monitoring?

eERDMS is administered by Department assigned users and a DOI contractor. The agreement with the contractor includes by reference Federal Acquisition Regulation (FAR) contract Clause 52.239-1, Privacy or Security Safeguards (Aug 1996). These regulations proscribe privacy protections including safeguards against unauthorized use of the data and unauthorized monitoring of individuals. Only authorized users will be able to access the system. In addition, all users must consent to the DOI Rules of Behavior and complete Federal Information System Security Awareness, Privacy and Records Management training before being granted access to the DOI network or any DOI system, and annually thereafter.

Any request to access DOI data made to the contractor supporting the operation or the assigned Departmental administrator. Access to eERDMS must be approved by the system owner or designated representative before access can be granted. Audit logs are used to ensure individual user access and actions are authorized and within the scope of official duties, and the user traceability program can detect and report unauthorized attempts to access files outside the scope of a user's permissions.

The audit log feature, unique identification, authentication and password requirements, along with mandatory security, privacy and records management training requirements, help prevent unauthorized monitoring, as well as unauthorized access to data, browsing and misuse.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

- ☒ Security Guards
- ☒ Key Guards
- ☒ Locked File Cabinets
- ☒ Secured Facility
- ☒ Closed Circuit Television
- ☐ Cipher Locks
- ☒ Identification Badges
- ☐ Safes
- ☐ Combination Locks
- ☐ Locked Offices
- ☒ Other. *Describe Cyber Locks*

(2) Technical Controls. Indicate all that apply.

- ☒ Password
- ☒ Firewall
- ☒ Encryption



- ☒ User Identification
- ☐ Biometrics
- ☒ Intrusion Detection System (IDS)
- ☒ Virtual Private Network (VPN)
- ☐ Public Key Infrastructure (PKI) Certificates
- ☒ Personal Identity Verification (PIV) Card
- ☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

- ☒ Periodic Security Audits
- ☒ Backups Secured Off-site
- ☒ Rules of Behavior
- ☒ Role-Based Training
- ☒ Regular Monitoring of Users' Security Practices
- ☒ Methods to Ensure Only Authorized Personnel Have Access to PII
- ☒ Encryption of Backups Containing Sensitive Data
- ☒ Mandatory Security, Privacy and Records Management Training
- ☒ Other. *Describe*

Audit logs, access level restrictions, and least privileges are used to ensure users have access only to the data they are authorized to view. In addition, firewalls and network security arrangements are built into the architecture of the system and NIST guidelines and Departmental policies are implemented for system and data security. System administrators will monitor the activities of authorized users to ensure that the system is properly used.

Additionally, the system uses a user traceability program that can detect unauthorized access attempts or access to files outside of their permissions. The audit trail features, unique identification, authentication and password requirements, and mandatory security, privacy and records management training requirement prevents unauthorized access to data, browsing and misuse.

All personnel must consent to DOI Rules of Behavior and complete annual mandatory security, privacy and records management training in order to receive and maintain access to the DOI network or systems.

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The eERDMS Information System Owner and system administrators are responsible for protecting individual privacy and will ensure that only authorized DOI and contractor employees can access the system. The Departmental Records Officer within the Policy Planning and



Management Division, Office of the Chief Information Officer serves as the eERDMS Information System Owner and the official responsible for oversight and management of the security and privacy controls for the information stored and processed in eERDMS. The Information System Owner is responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies and for protecting the privacy rights of the public and employees, and addressing privacy complaints in coordination with DOI privacy officials.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The eERDMS Information System Owner, Information System Security Officer, and System Administrators are responsible for ensuring the proper use of eERDMS. Authorized users are also responsible for ensuring the proper use of eERDMS, its components and data in accordance with Federal laws and policies. The eERDMS Information System Owner, Information System Security Officer and all authorized users are responsible for protecting individual privacy and reporting any potential compromise to DOI-CIRC, the Department's incident reporting portal, and DOI privacy officials in accordance with Federal policy and established DOI procedures. In accordance with the Federal Records Act, the Departmental Records Officer and bureau Records Officers are responsible for reporting any unauthorized records loss or destruction to NARA per 36 CFR 1230.